REMARKS

The above amendment and these remarks are responsive to the Office action, designated as FINAL, of 13 Jan 2005 of Examiner Linh L.D. Son.

Claims 1-22 are in the case, none as yet allowed.

35 U.S.C. 101

Claims 8, 9, 10, 11, 12, 16, 17, and 21 have been rejected under 35 U.S.C. 101.

The Examiner asserts that the language of these claims "raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment or machine."

These claims all relate to methods of operating hardware elements. Specific hardware elements are recited in these claims, as is their management. It is not a requirement that a program or software be recited to carry

out the steps of a method which is, as is the case here, carried out by clearly recited hardware elements.

However, in each of these claims, applicants have amended the preamble to make clear that the method steps are being executed by a digital processor at one end of a VPN connection. The hardware elements now recited include virtual private network (VPN) connections and a digital processor. The VPN connection, in particular, is clearly described in Applicants' invention as a hardware element. See Figure 2, and the description of VPN technology at page 2, lines 8-17 which clearly establishes the hardware nature, within the context of the Internet and computing industry, of the term VPN. Further, Claim 17 recites a database, VPN connections and address pools. A pool is a hardware element for storing addresses in an electronic database in an Internet environment, and this claim relates to configuring such a pool. See Applicants' Figure 2, element 48.

Applicants request, therefore, that the 101 rejection be reconsidered and withdrawn with respect to claims 8, 9, 10, 11, 12, 16, 17, and 21.

35 U.S.C. 103

Claims 1, 12, 13, 16, 18, 19 have been rejected under 35 U.S.C. 103(a) over Borella et al (U.S. Patent 6,353,614) in view of Jain et al. (U.S. Patent 6,047,325, hereinafter Jain).

Claims 2-7 have been rejected under 35 U.S.C. 103(a) over Borella et al in view of Jain et al, and further in view of Arrow (U.S. Patent 6,226,751).

Claim 11 is rejected under 35 U.S.C. 103(a) over Arrow.

Applicants traverse, and argue that the Examiner has not established a prima facie case of obviousness, for the reasons set forth hereafter.

Summary of The Present Invention

"IP security is provided in a virtual private network using network address translation (NAT) by performing one or a combination of the four types of VPN NAT, including VPN NAT type 'a source-outbound' IP NAT, VPN NAT 'b destination-

outbound', VPN NAT type 'c inbound-source' IP NAT, and VPN NAT type 'd inbound-destination' IP NAT. This involves dynamically generating NAT rules and associating them with the manual or dynamically generated (IKE) Security Associations, before beginning IP security that uses the Security Associations. Then, as IP Sec is performed on outbound and inbound datagrams, the NAT function is also performed." (Abstract)

The 4 types of VPN NAT are defined in another filing cited in END919990129, and also defined in the present application at p17, 5-19 (table 2). Applicants' invention concerns the ability to define and process multiple VPN NAT rules for a single VPN connection, via the specification of multiple IP addresses (an IP address set) for types of VPN NAT. The term 'VPN' here is used as a synonym for the IP Security protocols ESP (Encapsulating Security Payload) and AH (Authentication Header). Basic references for these protocols are (all from IETF (Internet Engineering Task Force)); IKE RFC2409 , ESP RFC2406, AH RFC2402, and the most basic, on IP Security architecture, RFC2401. Of course, Applicants' invention works over LANs and WANs, including wireless; it works wherever IP traffic works. And is embodied in *only 1 end* of the VPN connection; the VPN

implementation at the other end is completely unaware that its peer is performing VPN NAT operations. It *may* be embodied in both ends concurrently and independently, and this is a feature of Applicants' invention.

The problem addressed by Applicants' invention is that IP Sec & NAT are conflicting; a packet with IP Sec applied cannot, in any way, be altered without invalidating the packet. Yet NAT requires that parts of a packet be altered. How can these technologies be made to function together in an integrated fashion, so that the benefits of each can be concurrently obtained?

The key idea (in general terms) implicitly or explicitly included in all of Applicants' claims and that allows integration of VPN & NAT is that the NAT operation is logically performed *prior to beginning* the IKE negotiation of Security Associations, and is integrated with the start of IKE negotiations. Hence the IKE negotiation begins and proceeds with the NAT IP address(es), rather than actual IP address(es), and no additional steps or devices are required. Hence any possible IP Sec protocol that is applied to a datagram (encryption or digital signature or both) works at both ends, because both IKE (and the

resulting Security Associations) & IPsec are using the NAT address(es).

Following is a summary of how Applicants' invention differs from cited prior art in 6,353,614 (Borella et al), 6,047,325 (Jain et al), and 6,226,751 (Arrow et al);

For 6,353,614 (Borella et al); a method and protocol for Distributed NAT ("DNAT") is provided, used to overcome the limited 32-bit address space of IPv4. The protocol includes a port allocation protocol and translates ports as well as IP addresses. Local ports are replaced with globally unique ports, unique for the scope of DNAT. Hence, this invention employs what is often referred to as 'PNAT' meaning 'port & network [IP] address translation'. The problem Borella addresses is those they see as inherent in the current versions of NAT (col 1, 41-67, col 2, 1-28).

So, some of the differences between Borella et al Applicants' invention are;

a) Applicants' invention <u>does not translate port</u> (transport layer 'address') at all. The reason this is undesirable is because some classes of important IP

traffic do use TCP or UDP, hence the datagrams have no port numbers. These cannot be handled via a PNAT scheme. In contrast, Applicants' VPN NAT handles all IP protocol traffic.

b) DNAT is a form of PNAT that centralizes the assignment and allocation of ports. Borella et all has nothing to do with IP Security or the IP Security protocols ESP & AH. This is critical since the incompatibilities and difficulties of combining of IP Security & NAT are well known (see, for example, IETF RFC3715). Hence Borella et al does NOT even begin to address any of the problems associated with integrating IP Security and NAT. Nor is it a problem Borella is trying to solve.

c) Applicants' invention does not use PAP (Port Allocation Protocol) (col 5, 61-62) or anything similar to PAP. Applicants' invention does not allocate ports at all, using anything.

For 6,047,325 (Jain et al); a network device translates addresses and ports and filters packets at the link, network and transport layers. The Jain invention uses

a table (one of three mentioned) to bind MAC and IP addresses, via ARP (Address Resolution Protocol). The invention does say that traffic can be encrypted and authenticated when the traffic is sent over a wide-area-network. The problem Jain addresses is enabling a scalable virtual LAN (aka VLAN) over physical LANs and WANs.

Some differences between Jain et al and Applicants' invention are;

a) Applicants' invention does not translate ports (transport layer 'address') at all. The reason this is undesirable is because some classes of important IP traffic do use TCP or UDP, hence the datagrams have no port numbers. These cannot be handled via a PNAT scheme. In contrast, Applicants' VPN NAT handles all IP protocol traffic.

b) Applicants' invention does not need to translate IP address based on MAC addresses as does Jain, nor does it map IP addresses based on MAC addresses (at all) (col 6, 29-32).

c) Applicants' invention does not use APR or MAC addresses

at all. Hence Applicants' invention solves the functional combination of IPsec-based VPN and NAT in a manner completely different than Jain (if Jain solves it). This is illustrated by the observation that both ends of Jain et al (Fig 1, 26 & 28) must embody Jain et al, while for Applicants' invention, only 1 end of the peer VPN connection embodies Applicants' invention.

d) The mapping of MAC addresses to IP addresses to change apparent physical location of a IP address is the basic technology of VLANs. "If the packet is to be directed to a wide areas network, encryption and authentication procedures can be provided..." (col 2, 14-16). This and other passages in Jain suggest the relationship of Jain's use of VPN and Jain's use of network address translation (see for example important detail in col 5, 24-39). Note that 1st the packet is unencapsulated (a term commonly used in the context of VPN's) and then later (apparently optionally), a mapping to new MAC is made. In contrast, in Applicants' invention, NAT is integrated with IP Sec.

For 6,226,751 B1 (Arrow et al); a selection of a plurality of (network) entities to be coupled to a public

data network is done. The plurality is given identifiers. VPN's can be set up among the plurality that include encryption & authentication & compression. "Another variation on the embodiment includes defining address translation rules for virtual private network units coupled to the public data network" (abstract). The purpose if Arrow is to enable the realization of virtual private networks.

The following sections of Arrow are interesting; "The present invention is not limited to any one particular implementation technique" (col 4, 66-67). It goes on to say that one of ordinary skill in the are "will be able to implant the invention with various technologies without undue experimentation..." (col 5, 1-2). All this despite this: "... components implemented by the present invention are described at an architectural, function level", without details!

a) Applicants' invention does not need to select a plurality of entities coupled to the public data network.

b) Applicants' invention does not need to assemble a

plurality of identifiers for the plurality of entities.

c) Applicants' invention does not need to use these identifiers to identify communications between the entities.

d) Applicants' invention does not need to assemble the entities into groups.

e) It seems that (col 12, 7-54) that any IP Sec that Arrow might employ (no mention) is done before or after (some kind of) NAT for the communication, that is, serially. Hence NAT is not integrated with IP Sec.

f) Arrow uses port mapping (aka PNAT) (col 12, 52-54).

With respect to the current Office Action (AO);

For AO item 6, claims 1, 12, 13, 16, 18, 19 have been rejected under 35 USC 103(a):

For claim 1, differences between Borella and Applicants' invention are these --

Borella does not include "operating a virtual private network";

Borella does not include "configuring a NAT IP address pool";

Borella does not do "configuring a VPN connection to utilize said NAT IP address pool";

Borella does not do "obtaining a specific IP address from said NAT IP address pool, and allocating said specific IP address for said VPN connection";

Borella does not start "said VPN connection";

Borella does not do "loading to an operating system kernel the security association and connection filters for said VPN connection";

Borella does not process "a IP datagram for said VPN connection";

Borella does not do "applying VPN NAT to said IP datagram".

Since *none* of these parts of claim 1 are in Borella, Borella does not pertain to the subject matter of claim 1, and the entirety of these parts (i.e. Claim 1) would not have been obvious.

Continuing for claim 1, differences between Jain and Applicants' invention include the following -

Jain does not include "configuring a NAT IP address pool";

Jain does not do "configuring a VPN connection to utilize said NAT IP address pool";

Jain does not do "obtaining a specific IP address from said NAT IP address pool, and allocating said specific IP address for said VPN connection";

Jain does not do "applying VPN NAT to said IP datagram".

Since these parts of claim 1 are not in Jain, Jain does not pertain to this subject matter of claim 1.

Since Borella & Jain, taken as a whole, do not pertain to claim 1, claim 1 would not have been obvious to one of ordinary skill in art in light of Borella & Jain. This is also due to the fact that Borella & Jain seek to solve different problems than Applicants' invention. That is, combining a solution for problems with NAT (Borella) with a solution for virtual LANs (Jain) does not make obvious (or really, even relate to) integrating NAT with IP Sec in the manner described and claimed by Applicants.

With respect to claim 12 -

Borella & Jain do not teach "allowing a VPN NAT address pool to be associated with a gateway";

Borella & Jain do not teach "configuring a server NAT IP address pool for a system being configured";

Borella & Jain do not teach "storing specific IP addresses that are globally routable in said server NAT IP address pool";

Borella & Jain do not teach "configuring a VPN connection to utilize said server Nat IP address pool";

> Borella & Jain do not teach "managing total volume of concurrent VPN connections responsive to the number addresses in said server NAT IP address pool".

Since Borella & Jain, taken as a whole, do not to pertain to claim 12, or any part of claim 12, claim 12 would not have been obvious to one of ordinary skill in the art in light of Borella & Jain.

With respect to claim 13,

> Borella & Jain do not teach "a method of controlling the total number of VPN connections for a system based on availability of NAT addresses";
>
> Borella & Jain do not teach these "steps executed at one end of a VPN connection";
>
> Borella & Jain do not teach "configuring the totality of remote IP address pools with a common set of IP addresses, said addresses being configured as a range, as a list of single addresses, or any combination of multiple ranges and single addresses";

> Borella & Jain do not teach "limiting the successful start of concurrently active VPN connections responsive to the number of said IP addresses configured across the totality of said remote address pools."

Since Borella & Jain, taken as a whole, do not to pertain to claim 13, or any part of claim 13, claim 13 would not have been obvious to one of ordinary skill in the art in light of Borella & Jain.

With respect to claim 16,

> Borella & Jain do not teach "a system for operating a virtual private network (VPN) based on IP Sec that integrates network address translation (NAT) with IP Sec";
>
> Borella & Jain do not teach this "processing executed at one end of a VPN connection";
>
> Borella & Jain do not teach "means for configuring a NAP IP address pool";
>
> Borella & Jain do not teach a "means for configuring a

VPN connection to utilize said NAT IP address pool";

Borella & Jain do not teach a "means for obtaining a specific IP address from said NAT IP address pool, and allocating said specific IP address for said VPN connection";

Borella does not teach "means for starting said VPN connection";

Borella & Jain do not teach "means for loading to an operating system kernel the security associations and connection filters for said VPN connection";

Borella & Jain do not teach "means for applying VPN NAT to said IP datagram" (p11, 36).

Since Borella & Jain, taken as a whole, do not to pertain to the above recited limitations set forth for claim 16, claim 16 could not have been obvious to one of ordinary skill in the art in light of Borella & Jain.

For claim 18,

Borella & Jain do not teach "a system implemented at one end of a VPN connection for allowing a VPN NAT address pool to be associated with a gateway, thereby allowing server load-balancing";

Borella & Jain do not teach "a server NAT IP address pool configured for a given system being configured for containing multiple addresses configured as a range, as a list of single addresses, or any combination of multiple ranges and single addresses";

Borella & Jain do not teach "said server NAT IP address pool storing specific IP addresses that are globally routable";

Borella & Jain do not teach "a VPN connection configured to utilize said server NAT IP address pool";

Borella & Jain do not teach "a connection controller for managing total volume of concurrent VPN connection responsive to the number of addresses in said server NAT IP address pool".

Since Borella & Jain, taken as a whole, do not to pertain to

claim 18, or any part of claim 18, claim 18 could not have been obvious to one of ordinary skill in the art in light of Borella & Jain.

For claim 19,

Borella & Jain do not teach "a program storage device readable by a machine ... to perform method steps executed at one end of a VPN connection for operating a virtual private connection (VPN) based on IP sec that integrates network address translation (NAT) with IP Sec processing";

Borella & Jain do no teach "configuring a NAT IP address pool" (p13, 83);

Borella & Jain do not teach "configuring a VPN connection to utilize said NAT IP address pool" (p13, 85-86);

Borella & Jain do not contain "obtaining a specific IP address from said NAT IP address pool, and allocating said specific IP address for said VPN connection" (p13, 88-90); Borella & Jain do not contain "applying VPN NAT

to said IP datagram" (p 13, 100).

Since Borella & Jain, taken as a whole (that is, in combination), do not contain significant parts of claim 19, claim 19 could not have been obvious to one of ordinary skill in the art in light of Borella & Jain.

For AO item 7, claims 1, 12, 13-16, 18, 19, 20 and 22 as per "the previous office action rejection basis is maintained". The previous office action listed "1, 12, 13, 16, 18, 19 and 22" (previous AO item 7), not the "13-16" listed in the current AO. First we respond in detail to the previous AO item 7.

Borella (col 6 lines 27-38) are cited for "includes the obtaining a specific private IP form the ... NAT IP pool". The previous AO goes on to state "However, Borella et al do not teach the implementation of ... VPN with ... IP Sec with NAT". The cited passage concerns the association of PAP with the DHCP & BOOTP protocols: "... a network device transmits PAP request message 66 upon boot. In such an embodiment, PAP 64 can be associated with Dynamic Host Configuration Protocol ('DHCP') or ... ('BOOTP')." Then

Jain is referenced (col 5, 25) as also using DHCP.

But, Applicants' invention does not use, and does not require DHCP, Hence the combination of Borella & Jain and their use of DHCP has no bearing on Applicants' invention, and does not make Applicants' invention obvious to one of ordinary skill in the art.

The previous AO item 7 goes to say "It is obvious at the time of the invention was made for one of ordinary skill in the art to incorporate IP Sec with NAT (Jain col 5, 6-9) and Borella (col 16, 7-24 and fig 13 176 and 178) to protect against both internal and external security breaches."

The Jain citation concerns mapping IP addresses to MAC addresses (using one of Jain's three tables) (Jain fig 6, 112, 126). The Borella citation concerns Borella's view advantages of their DNAT and ends with stating that DNAT 'can also be used to support VPN's' (Borella, col 16, 22-23). The cited figure and figure items concern setting IP addresses in an inner and outer IP header, and with translating a "local source port ... to a globally unique port". Hence the AO position can be paraphrased like this: It is obvious at the time of the invention was made for one

of ordinary skill in the art to incorporate IP Sec with NAT <using or dealing with mapping IP address to MAC addressees> and <because DNAT has advantages over regular NAT> and <having inner and outer IP headers and translating a local port to a globally unique port>. Restated with substance rather than citation makes it clear that it is not at all obvious, and in fact, does not even have bearing on the integration of IP Sec and NAT.

To further make this apparent; using or dealing with mapping IP address to MAC addresses is irrelevant to Applicants' invention (since Applicants' invention does not do this). The advantages of DNAT over regular NAT are irrelevant to Applicants' invention (since Applicants' invention does not use DNAT, nor does it translate port numbers). And finally translating a local port to a globally unique port is irrelevant to Applicants' invention (since the integration of NAT with IP Sec does not use port translation). Hence these irrelevant capabilities do not combine to make obvious the integration of IP Sec with NAT.

The previous AO item 7 finishes with "In claims 12 and 13, it is obvious at the time of the invention was made for one of ordinary skill in the art to recognize that the

number of connections is limited to the IP address pool."

In claim 12, the point is made that load-balancing is enabled, not only limiting the number of connections based on the IP address pool. The larger point is that new capabilities are enabled by integrating NAT with IP Sec, and not only is the integration of NAT with IP Sec non-obvious, but the ennoblement of such a capability as in claim 12 is non-obvious. Neither Borella nor Jain contain any such capability.

Again, claim 13 shows a new capability based on the integration of NAT with IP Sec, namely the "limiting the successful start of concurrently active VPN connections...", based on the VPN NAT pools. Since the VPN NAT pools are a non-obvious feature of Applicants' invention which integrates IP Sec and NAT, this further capability is non-obvious.

Returning to the current AO item 7, it goes on to state "the implementation of NAT with VPN connection has also been considered in Borella ... (col 16, lines 20-23)". The cited text merely says "Illustrative embodiments of the present invention can also be used to support VPNs". There

is no detail, no specifics, no elaboration anywhere in Borella on what this means or how it might be accomplished. The problem of integrating NAT with IP Sec is not described or solved. More specifically, Borella does not teach "a method of operating a VPN based on IP Sec that integrates ... NAT with IP Sec processing" (claim 1). In addition, Borella does not teach "the steps executed at one end of a VPN connection" of "configuring a NAT IP address pool" ... "loading to an operating system kernel the security associations and connection filters for said VPN connection".

The (current) AO item 7 goes on to say that Jain teaches VPN connection setup utilizing DHCP servers; indeed it does. Applicants' invention does not use, nor require, nor cite DHCP servers for any use. The reason is because DHCP servers are irrelevant to Applicants' invention.

The AO then says "... it would be obvious ... to incorporate Borella's NAT method with Jain's VPN connection method...". Applicants traverse this assertion, because the distributed NAT of Borella is very different in numerous key features from VPN NAT, as previously described. In addition, Borella's DNAT has little or nothing to do with IP

Sec. For example the "protocol includes a Port Allocation Protocol (PAP) for allocating globally unique port numbers ... . (col 2, 34-36). And the "... network device uses a combination network address (e.g. common external network address / globally unique port number) for communications..." (col 2, 46-49). And, "the method and protocol distribute network address translations to individual network devices on a network..." (col 2, 50-51).

Applicants' invention, and VPN NAT, does none of these things; no PAP, no allocation of globally unique port numbers, no use of combination network address, and no distributing of network translations. Hence the DNAT of Borella is a very different form of NAT than VPN NAT, and therefore it would not have been obvious to use DNAT to achieve the capabilities of VPN NAT.

Similarly, Jain has a "network device that translates addresses of machines ... and filters packets at the link, network and transport layers" (col 1, 65-67). Jain uses "an address resolution protocol" (col 2, 54-55). Jain has "a mapping table for mapping network addresses at the network layer of machines on the second local area network

to the media access control address of the network device on the first local area network" (col 6, 29-32). Note the 'addresses of machines' refers to MAC addresses, not IP addresses.

Applicants' invention does not employ MAC address translation, nor does it filter packets at the link or transport layers. Applicants' invention does not use ARP (address resolution protocol). Applicants' invention does not use a mapping table to map network addresses to MAC (media access control) addresses. And, while Jain does mention encryption and authentication, is does not specifically refer to the IP Sec protocol suite, and Internet Key Exchange (IKE) protocol, all standardized by the IETF and used in Applicants' invention.

Hence there are many significant differences between Jain and Applicants' invention. The kinds of address translations Jain employs are very different from VPN NAT, and Jain does give any specifics about how its kinds of translations are use with Jain's encryption & authentication, which may be different than IP Sec.

Hence the combination of Borella's DNAT and Jain's NAT

do not make obvious to one of ordinary skill in the are how to integrate VPN NAT with IP Sec.

The current AO item 7 (last sentence) says "The incorporation of NAT in Jain's DHCP server would allow the VPN connection to be executed on one end of the connection (Borella col 16 lines 20-23 and Jain col 5, lines 13-40)". Applicants traverse.

As noted earlier, DNAT includes port translation (Borella col 16, 13-14) and VPN NAT does not. As noted earlier, DHCP is irrelevant to Applicants' invention. (DNS is also irrelevant to Applicants' invention.) As noted earlier, there are many other differences between Applicants' invention and Borella's DNAT, and Jain's various translations. Further, VPN (as used in Applicants' invention) cannot "be executed on one end of the connection" because of the definition of the underlying ESP and AH protocols (aka IP Security protocols; see IETF RFC's referenced above). And, this is not what Applicants' invention claims. It claims (claim 1, for example) "a method of operating a VPN based on IP Sec that integrates ... NAT with IP Sec processing comprising the steps executed at one end of a VPN connection" (p4, 1-5). It is the

integrated operation of VPN NAT that operates at one end of the VPN connection, not IP Sec (or "VPN") itself. This can be considered another example of how Applicants' invention is not obvious to one having ordinary skill in the art.

As a further illustration of the points above, Applicants' invention claim 12 recites, "a method to allow a VPN NAT address pool to be associated with a gateway, thereby allowing server load-balancing comprising the steps executed at one end of a VPN connection". Neither Borella nor Jain have a VPN NAT address pool, neither mention load-balancing, and neither use VPN NAT and the steps executed at one end of a VPN connection. Borella and Jain do not contain "configuring a server NAT IP address pool for a system...". Borella and Jain do not contain "storing specific IP addresses that are globally routable in said server NAT IP address pool". Borella and Jain do not contain "configuring a VPN connection to utilize said server NAT IP address pool". Borella and Jain do not contain "managing total volume of concurrent VPN connections responsive to the number of addresses in said server NAT IP address pool."

For current invention claim 13, Borella & Jain do not

contain "a method of controlling the total number of VPN connections" (p8, 74-75). And Borella & Jain do not contain the 2 clauses of claim 13.

For Applicants' claim 16, Borella & Jain do not contain "a system for operating a VPN based on IP Sec that integrates NAT with IP Sec processing executed at one end of a VPN connection" (p10, 13-16). Borella & Jain also do not contain the steps in claim 16.

For Applicants' claim 18, Borella & Jain do not contain "a system implemented at one end of a VPN connection for allowing a VPN NAT address pool to be associated with a gateway, thereby allowing server load-balancing" (p12, 54-57). Borella & Jain also do not contain the steps listed in claim 18.

For Applicants' invention claim 19, Borella & Jain do not contain "a program storage device ... to perform method steps executed at one end of a VPN connection for operating a virtual private network (VPN) based on IP Sec that integrates network address translation (NAT) with IP Sec processing". Borella, Jain or the combination of Borella & Jain do not contain "configuring a NAT IP address pool",

"configuring a VPN connection to utilize said NAT IP address pool", "obtaining a specific IP address from said NAT IP address pool, and allocating said specific IP address for said VPN connection", "starting said VPN connection", "loading to an operation system kernel the security associations and connection filters for said VPN connection", "processing a IP datagram for said VPN connection", and "applying VPN NAT to said IP datagram".

Similarly for claims 20 & 22. That is, neither Borella, Jain, nor the combination of Borella & Jain, contain the following; "... VPN based on IP Sec that integrates NAT with IP Sec processing", "... executed at one end of a VPN connection", "... means for causing a computer to effect configuring a NAT IP address pool", "... configuring a VPN connection to utilize said NAT IP address pool", "... obtaining a specific IP address from said NAT IP address pool, and allocating said specific IP address for said VPN connection", "... to effect starting said VPN connection" (p15, 26), and so on, for the remaining clauses.

For AO item 8, claims 14 & 15, claim 1 rejection basis is incorporated: Claim 14 makes the point that even though NAT & IP Sec are occurring, ICMP datagrams are correctly and

successfully handled by Applicants' invention. This can be done in part because port translation is not used, and because Applicants' invention also translates the IP addresses that are internal to the ICMP packets (various types).

With respect to claim 14, as noted earlier, Borella translates ports. Perhaps confusingly, Borella's Port Allocation Protocol is (or can be) implemented using ICMP (col 5, 62-63). However, DNAT itself cannot be applied to ICMP traffic, since they have no ports, because they have no transport protocol header. (ICMP refers to Internet Control Message Protocol; please refer to IETF RFC0792 and RFC2463.) Hence Borella is irrelevant to claim 14.

Concerning claim 15; it basically says that the combination of IP Sec and NAT in VPN NAT correctly and successfully handles FTP (File Transfer Protocol (RFC)0959) traffic. In fact, VPN NAT overcomes the problems alluded to in the cited Borella reference (col 2, 22-28), for FTP. Far from overcoming them, Borella uses these problems to explain why DNAT is valuable! Hence Borella cannot teach claim 15.

For AO item 9, claims 2-7 are rejected under 35 USC 103(a), over Borella, in view of Jain, and further in view of Arrow.

As has been seen elsewhere in this response, Borella, in view of Jain does not imply or suggest VPN NAT to one of ordinary skill in the art, due to the many differences between Applicants' invention and Borella (which does not relate to VPN at all), Jain (which includes MAC to IP address mapping, not VPN NAT). In adding consideration of Arrow there is a superficial relationship to Applicants' invention in that Arrow claims using NAT in a VPN context (col 12, 8-24). However, Arrow does not claim any integration of NAT with IP Sec, does not specify the protocol basis for its VPNs (may or may not be IP Sec), and does not provide any details about how NAT is used with VPN.

The integration of NAT with IP Sec-based VPN is a key to Applicants' invention, and this is present in all claims and described though out the filing. See for example p17 Table 1 and its description which defines one aspect of the integration of NAT with IP Sec, using the IKE protocol nomenclature. Also, Arrow makes no mention of a VPN NAT pool.

In particular, Arrow does not claim "the method of claim 1, wherein said VPN connection is configured for outbound processing, and said applying step comprises outbound source IP NATing" (Applicants' claim 2).

For claim 3, the totality of Borella, Jain and Arrow do not contain "the method of claim 1, wherein said VPN connection is configured for some combination of inbound processing, and said applying step selectively comprises inbound source IP NATing or inbound destination IP NATing."

Claims 2 & 3 concern three particular types of VPN NAT, as defined in the filing, and captured in table 1, p17 and associated text.

In Applicants' invention, claim 4, the point is made that VPN NAT may be used with manually-keyed IP Sec connections. No mention is made of any such VPN connections in the whole of Borella, Jain and Arrow.

In Applicants' invention, claim 5, the point is made that VPN NAT may be used with dynamically-keyed IP Sec connections. No mention is made of any such VPN

connections in the whole of Borella, Jain and Arrow.

In Applicants' invention, claim 6, the point is made that VPN NAT may be used with IKE-based dynamically keyed IP Sec connections, "wherein said starting step further comprises creating a message from IKE containing said IP address from said NAT pool" (p6, 4-6). Nothing like this is mentioned in the whole of the whole of Borella, Jain and Arrow.

In Applicants' invention, claim 7, the point is made that VPN NAT may be used with IKE-based dynamically keyed IP Sec connections, "... keys with said NAT pool IP address wherein said loading step loads the result as security associations into said operating system kernel" (p6, 12-14). Nothing like this is mentioned in the whole of Borella, Jain and Arrow. They do not even mention security associations, a key concept in IP Sec VPN's, and they do not mention VPN NAT pool derived IP address in conjunction with the security association.

All of these differences between Applicants' invention and Borella, Jain & Arrow are part of why Applicants' invention non-obvious to one of ordinary skill in the art.

For AO item 10, claims 2-7 "the previous written action rejection basis is maintained and further incorporated the obviousness rejection of claim 1. Applicants traverse: the previous AO rejection of 2-7 is identical to current AO item 9, above.

For AO item 11, claim 11 is rejected under 35 USC 103(a) ... over Arrow (6,226,751). Applicants traverse: Arrow does not contain "a method of providing customer tracking of VPN NAT activities as they occur in an operating system kernel, comprising the steps executed at one end of a VPN connection" (p7, 43-46). Arrow also does not contain anything like "responsive to VPN connection configuration, generating journal records", nor "updating said journal records with new records for each datagram processed through a VPN connection" (p8, 51-52), nor "enabling a customer to manage said journal records".

For AO item 12, claim 11 "the previous written action rejection basis is maintained". Applicants traverse. In the previous AO item 14 is stated that 'Arrow discloses a method of providing customer tracking of VPN NAT activities (col 10, lines 17-20)', which states "Simple Network

Management Protocol (SNMP) module 720 gathers information and statistics from IP stack 712 that a system administrator might be interested in, such as communication traffic statistics." Applicants traverse. SNMP is a very well know and very well established system management protocol, particularly in the network area. And it quite simply does none of what is in claim 11. This is the case despite the previous AO's statement that 'It is obvious at the time of the invention was made for one of ordinary skill in the art to recognize that the same protocol includes the claim feature completely'. In fact SNMP most definitely (at the time of the invention) did not include the claim feature; this can be seen by examining the SNMP MIB's that are defined by the IETF, in particular , any MIB's that relate to IP Sec, IKE, etc.. (There do not appear to be any SNMP MIBs specific for IKE, IP Sec, NAT or VPN. However, for reference here is a list of some possibly related RFC's, RFC2667, RFC2720, RFC2465, and the RFC that defines the MIB for IPv4.)

For AO item 14, "Borella does utilize P NAT and D NAT...". Applicants traverse. DNAT is simply Borella's abbreviation for 'Distributed NAT' (col 2, 30-34), which uses Borella's PAP (Port Allocation Protocol) for allocating

globally unique port numbers (col 2, 30-41). 'PNAT' is a fairly common industry term for 'port and network address translation'. It is irrelevant that Borella uses PNAT since VPN NAT does not translate ports. And the fact that Borella calls his method DNAT is irrelevant to VPN NAT. The point is that Borella translates ports and Applicants' invention does not, and does not need to. In contrast, port translation is clearly central to Borella.

The AO states "further, Borella does anticipates the implementation of DNAT in the VPN environment...". In fact Borella mentions VPN's rarely, for example in a single sentence in col 16, 22-23. This of course must be taken on faith since no specifics are given concerning how DNAT "can be used" to support VPN, and the underlying technical problems are entirely ignored. Even if the specifics were supplied, the fact that DNAT is used with its port translation means it is not VPN NAT. And further Applicants' invention integrates VPN NAT with IP Sec, and claims the details on how this is accomplished.

Note that Borella also implicitly alludes to VPN (and perhaps, IP Sec-base VPN) in col 1, lines 51-52, when he acknowledges that 'this type of NAT' (meaning normal NAT)

"causes security problems by preventing certain types of encryption from being used"! The integration of VPN NAT with IP Sec is meant to solve just this kind of problem.

For AO item 15, "As regarding to Jain, Applicant argues that Jain teaches port translation, utilizes ports and MAC addresses, and the claimed invention does not. However, the nowhere in the claim language recites the limitation and clearly explains otherwise. Therefore, Jain's invention reads directly in the claim with the incorporation of Borella invention."

It is true that specifics regarding the lack port translation are not in the claim language as a limitation, because it is not central to the idea of integrating NAT with IP Sec (hence 'VPN NAT'). In fact VPN NAT could employ port translation; but its not necessary. Whereas in Borella, port translation is central, because Borella is solving a different problem. So combining the problem solved by Borella with Jain does not solve or even suggest Applicants' invention. The reason is that neither Borella nor Jain address how NAT can be integrated with IP Sec (naturally; it would not be expected given the problem each was addressing) and further, the integration is non-obvious

to one of ordinary skill in the art, due to the many differences between Borella, Jain, and Borella combined with Jain, and Applicants' invention.

Applicants request, therefore, that the rejection of claims 1-22 under 35 U.S.C. 103 be reconsidered and withdrawn.

SUMMARY AND CONCLUSION

Applicants urge that the above amendments be entered and the case passed to issue with claims 1-22.

The Application is believed to be in condition for allowance and such action by the Examiner is urged. Should differences remain, however, which do not place one/more of the remaining claims in condition for allowance, the Examiner is requested to phone the undersigned at the number provided below for the purpose of providing constructive assistance and suggestions in accordance with M.P.E.P. Sections 707.02(j) and 707.03 in order that allowable claims can be presented, thereby placing the Application in

condition for allowance without further proceedings being necessary.

Sincerely,

E. B. Boden, et al.

By

Shelley M Beckstrand
Reg. No. 24,886

Date: 14 Mar 2005

Shelley M Beckstrand, P.C.
Attorney at Law
61 Glenmont Road
Woodlawn, VA 24381-1341

Phone: (276) 238-1972
Fax: (276) 238-1545